

Network Management 2

Reading:

Leinwand, A. & Conroy, K. F. (1996) Network Management: A Practical Perspective 2nd ed. Addison-Wesley. Chapters 3 to 7.

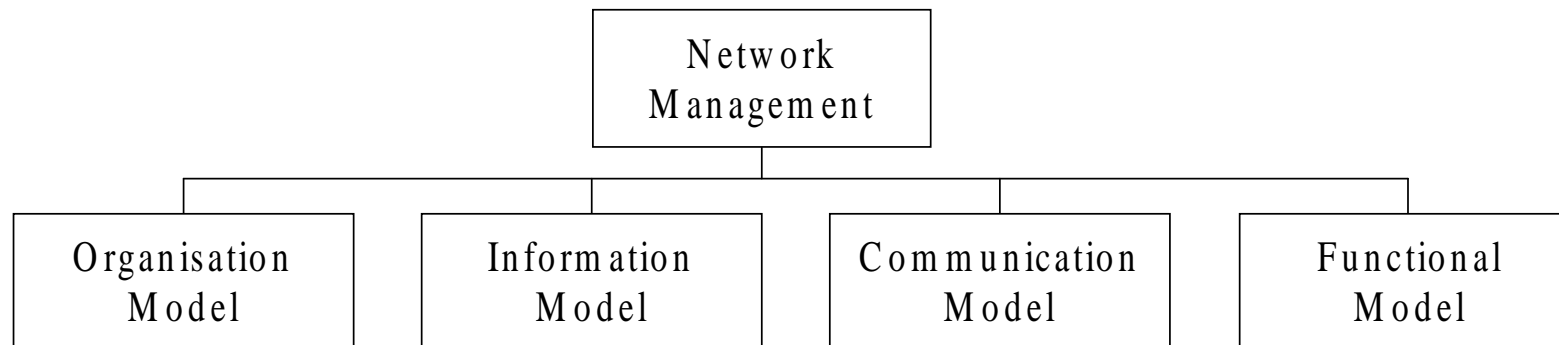
Stevenson, D. W. (1995) Network Management What it is and what it isn't.
<<http://www.sce.carleton.ca/netmanage/NetMngmnt/NetMngmnt.html>> [Accessed September 20 2005]

Cisco Systems (2004) Network Management System: Best Practices White Paper.
<http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml>
[Accessed September 20 2005]

Cisco Systems (2002) Network Management Basics.
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm>
[Accessed September 20 2005]

OSI Network Management Model

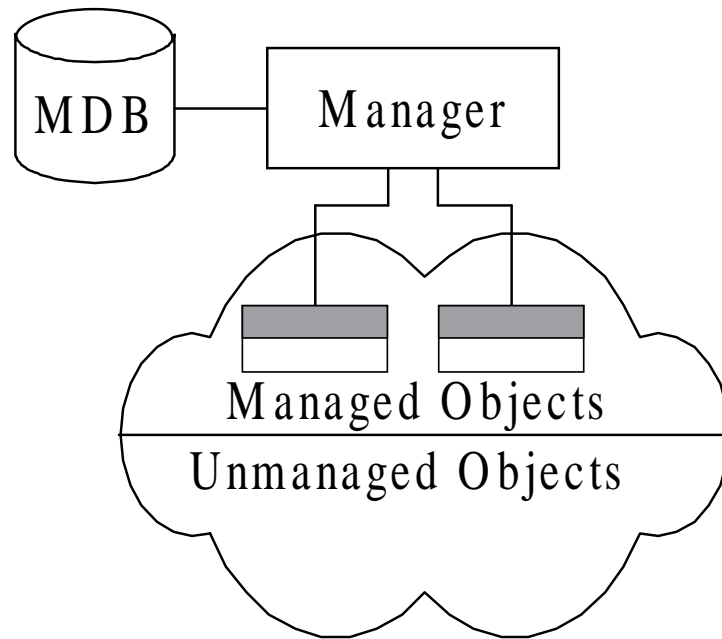
The OSI “architecture” comprises of four models



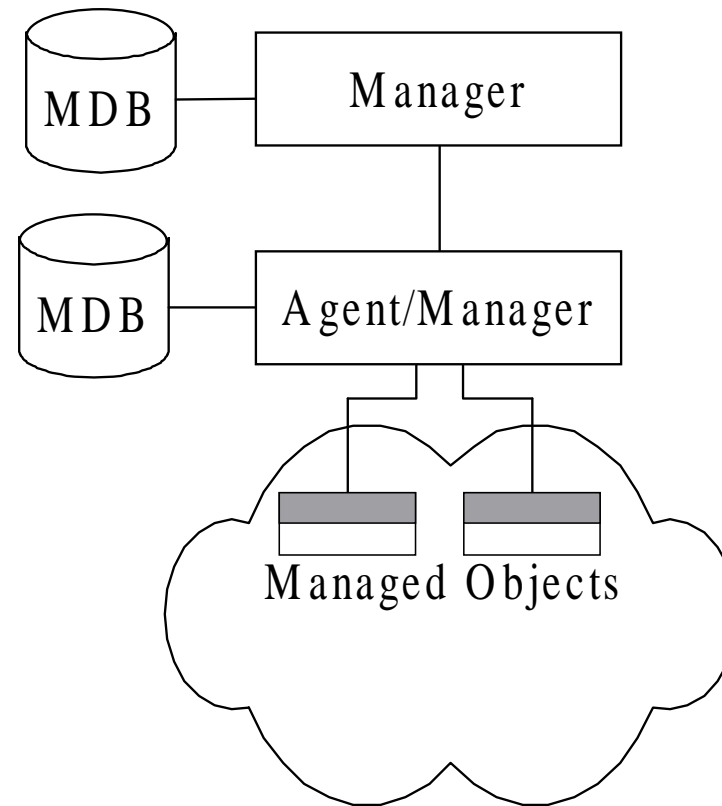
Organisation Model

- Defines the components of a network management system, their functions and their relationships.
- Defined in OSI 10041 — Systems Management Overview. It defines the terms such as *object*, *agent* and *manager*.
- Network objects consist of network elements such as hosts, hubs, bridges, routers etc. They can be managed or unmanaged.
- Managed objects have a management process called an agent running in them. Manager queries agent, receives back management data, processes it and stores it in its database.
- The agent can send a minimal set of alarm information to the manager unsolicited.

Two and three tier models



Two-Tier Network Management
Organisation Model

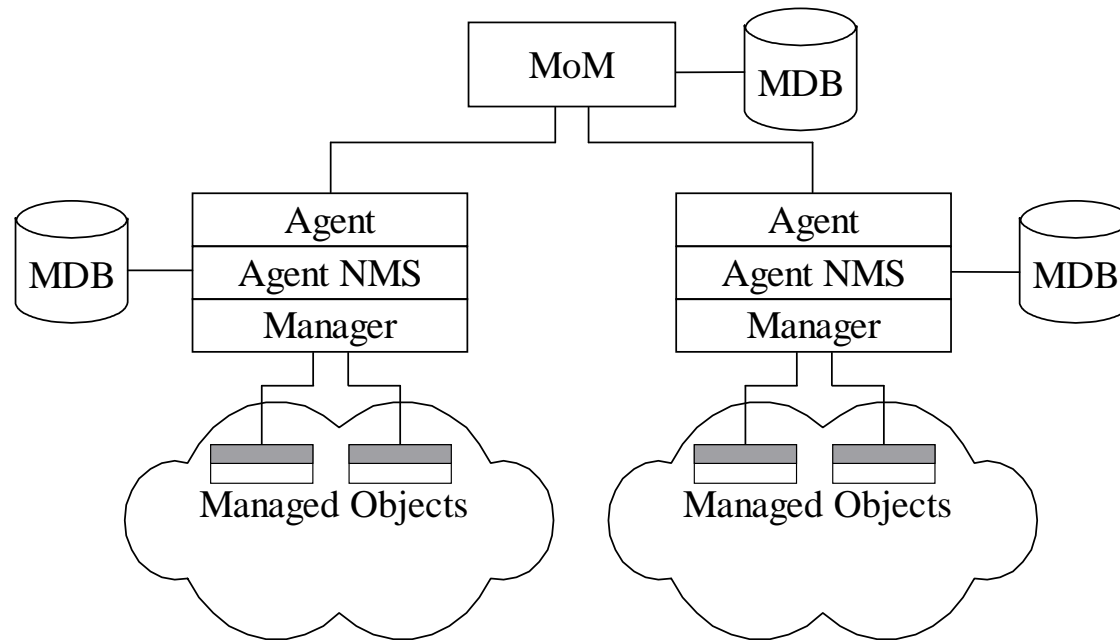


Three-Tier Network Management
Organisation Model

- In the two tier model there is a clear distinction between the manager and the managed objects.
- In the three tier model there is an intermediate layer that acts as both agent and manager. As manager, it collects data from the network elements, processes it, and stores the results in its database.

As agent, it transmits information to the top-level manager. e.g. an intermediate system is used for making statistical measurements on a network and passing the information as needed to the top level manager.

Networks can be managed locally and a global view of the networks can be monitored by a manager of managers.



Network Management Organisation Model with Manager of Managers

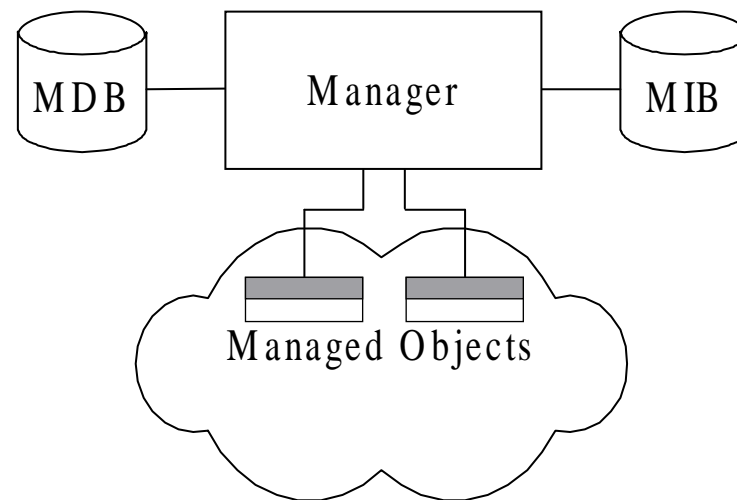
Network management systems can also be configured as peer-to-peer relationships.

Information Model

- Concerned with the structure and storage of information.
- Specifies the information base to describe managed objects and their relationships. ISO 10165 specifies the **Structure of Management Information (SMI)** and the information database, **Management Information Base (MIB)**.
See rfc 1155 for the **SMI** and rfc 1213 for **MIB-II**.
- The MIB is used by both agent and management processes to store and exchange management information.
- MIB associated with an agent MIB called the agent MIB and the MIB associated with a manager is called the manager MIB.
- A manager MIB consists of information on all the network components that it manages.
- An agent need only to know its local information — its MIB view.

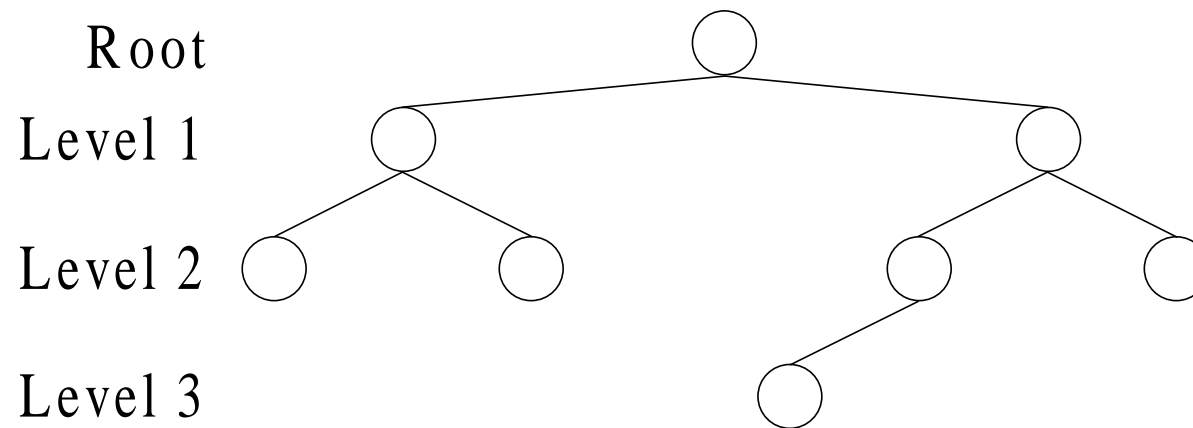
Difference between the Management Database (MDB) and the MIB

- The MDB is a real database and contains the measured or administratively configured values of the elements of the network.
- The MIB is a virtual database and contains the information necessary for processes to exchange information.



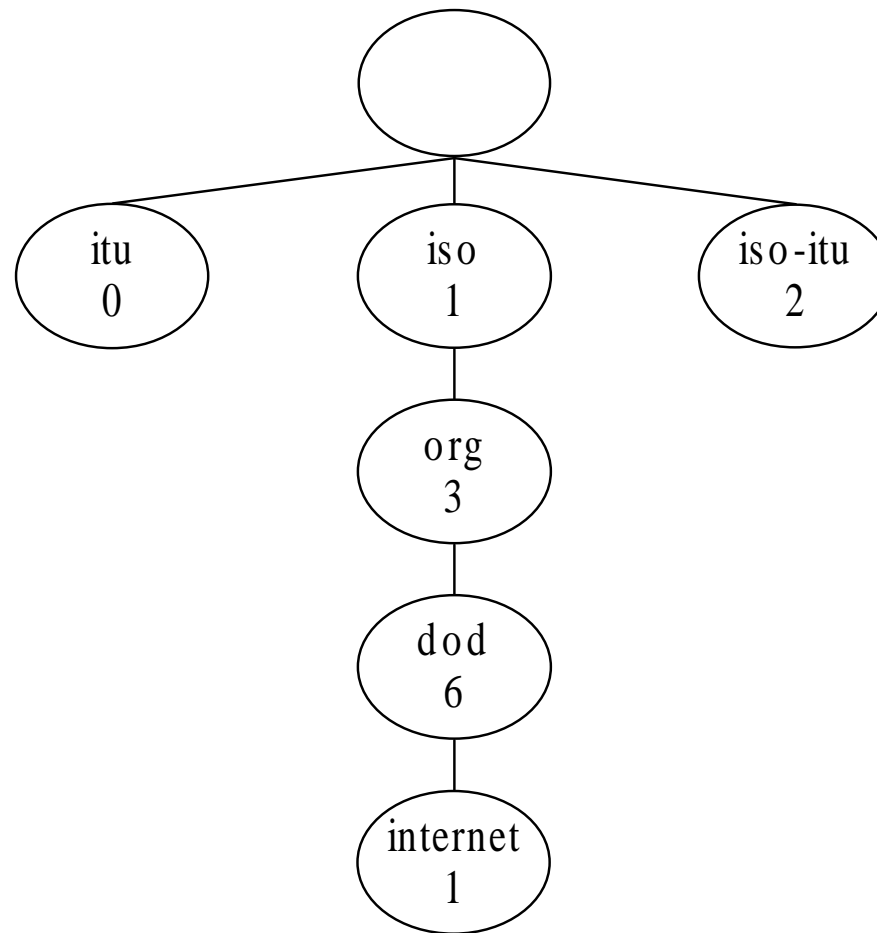
Management Information Trees

Managed objects are uniquely defined by a tree structure specified by the OSI model that is also used in the Internet model.



Generic Management Information Tree

- There is a root node and well defined nodes underneath each node at different levels.
- Each managed object occupies a node in the tree.

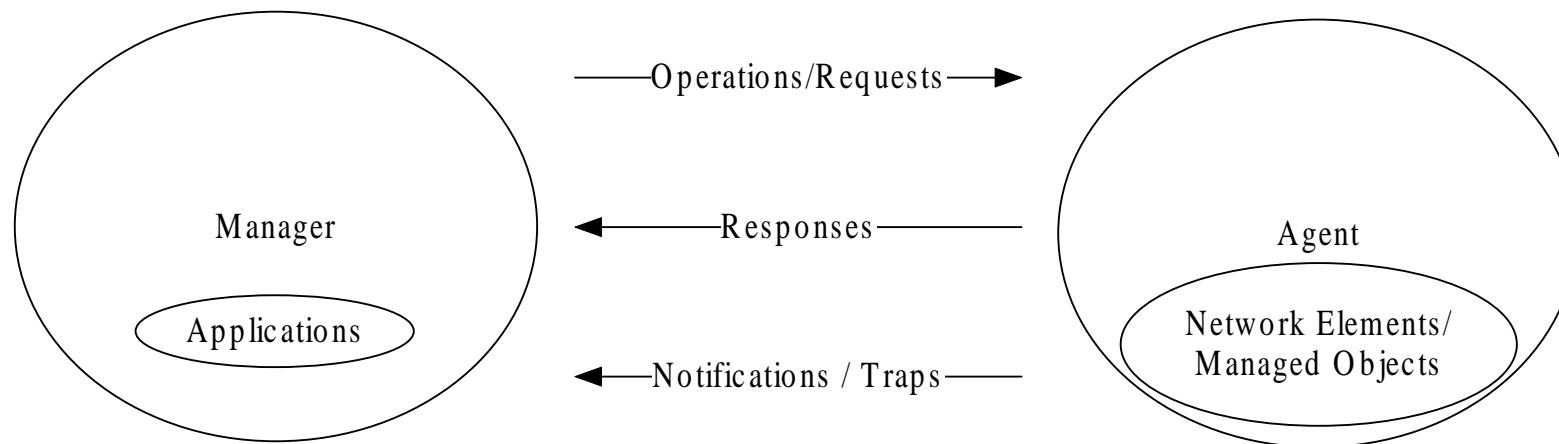


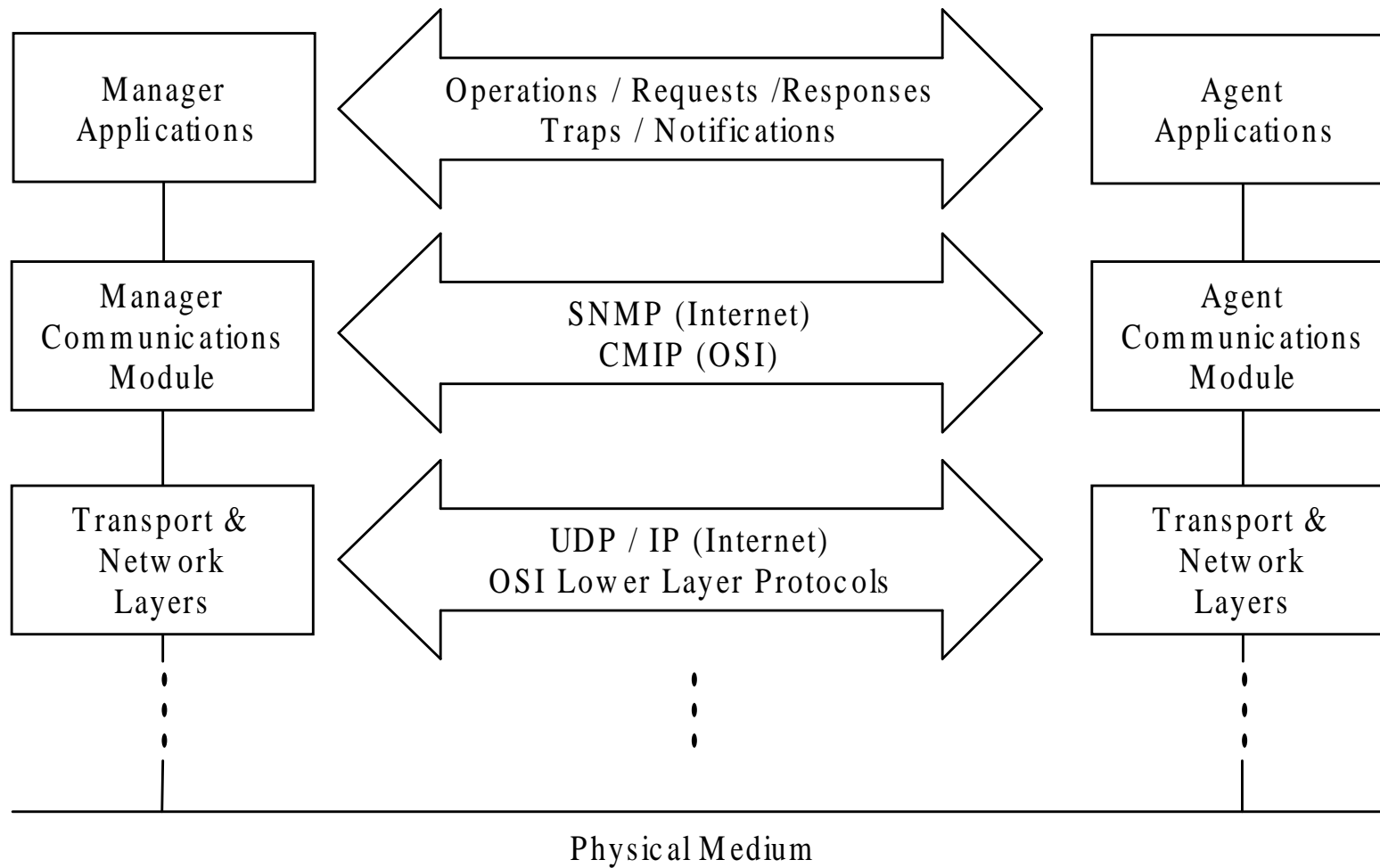
OSI Management Information Tree

- There are three nodes in the layer beneath the root **iso**, **ccitt (itu)**, and **iso-ccitt (iso-itu)**.
- The two standards organisations are on the first layer and define managed objects under them.
- The joint node is for objects jointly defined by the two organisations.
- The number in each node identifies the designation of the object in each layer.
So **iso** is **1**, **org** is **1.3** and **dod** is **1.3.6**.
All Internet managed object thus begin with **1.3.6.1**.

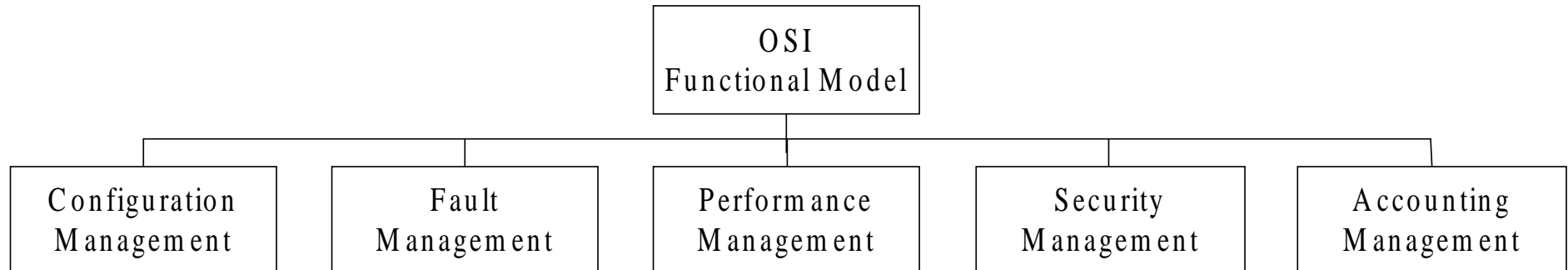
Communications Model

- Deals with the way information is exchanged between systems.
- Three aspects need to be addressed:
transport protocol,
message format for communication (application protocol)
and the actual messages.





Functional Model



ISO 7498-4 defines five functional management areas.

- Fault, Configuration, Accounting, Performance, Security.
- Easily remembered by the acronym FCAPS.
- Can be broken down into two broad areas – monitoring and control.

Control Functions

- **Configuration**

Determining and setting the configuration of devices.

Normally used in discovering network topology, mapping the network and setting up configuration parameters in management agents, and management systems.

e.g. use of broadcast ping or examination of the arp caches local routers.

Note: auto discovery with VLANs is a much more complex process.

In a broad sense configuration management also covers network provisioning which includes network planning and design. Network provisioning is based on performance statistics and quality of service requirements.

- **Security**

Controlling access to network resources, including information stored and being transferred, according to a well-defined security policy.

Identify that which is to be protected.

Find the access points.

Secure the access points.

Maintain the secure access points.

Monitoring Functions

- **Fault**

Detection, isolation, response — correction (if possible), logging.

Immediate handling of transient network failures e.g. link, host or router hardware or software outages.

Detection → location, service restoration → identification of root cause → problem resolution.

Self-healing.

Trouble-tracking systems – trouble tickets. Each “ticket” records data about a problem and the actions taken when dealing with it from start to finish. Could be part of a sophisticated network management tool that works in conjunction with an expert system.

Fault detection is accomplished either by polling or the generation of traps.

e.g polling – a fault management application generates a ping periodically and waits for a response. When a preset number of responses are not received connectivity is declared broken.

The advantage of traps over polling is that failure detection is accomplished faster with less traffic overhead.

- **Accounting**

Specifying, logging and controlling user and device access to network resources.
Gathering statistics in order to make decisions about the allocations of network resources. e.g. querying activity logs on individual hosts or traffic counters from network devices such as bridges, routers and switches.

Frequency of gathering such statistics depends upon the amount of activity and the fact that SNMP counters can hold values up to $2^{32} - 1 = 4\,294\,967\,295$.

- **Performance**

Quantify, measure, report, analyse and control the performance of different network components.

Data traffic management.

Involves data monitoring, problem isolation, performance tuning, statistical trend analysis and resource planning.

Performance parameters: throughput, response time, network availability and network reliability.

Parameters affecting throughput: capacity of media, utilisation, channel error rate, peak load, average traffic load.

Network Monitoring Calculation Example 1

A network administrator wishes to monitor 5000 workstations to see whether they are switched on or not. In order to do this each machine is periodically pinged. The message size in both directions is 174 bytes. This **includes** 20 bytes of IP. The administrator's NMS (network management station) is on a 10 Mbps 802.3 switched LAN operating in half-duplex. If each machine is pinged every 50 seconds determine the maximum percentage of the capacity of the LAN connection that is being used in monitoring the workstations.

Total number of bytes each way = $174 + 26 = 200$ bytes.

Time taken to transmit 200 bytes = $\frac{200 \times 8}{10 \times 10^6} = 0.16 \times 10^{-3} \text{ s} = 0.16 \text{ ms}$.

So time taken to send and receive a ping = 0.32 ms.

Time required to monitor 5000 workstations once = $5000 \times 0.32 \times 10^{-3} = 1.6 \text{ s}$.

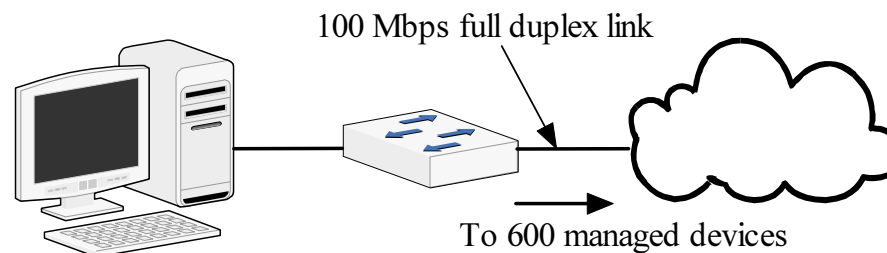
Note: this ignores the inter-frame gap of $9.6 \mu\text{s}$ in 10 Mbps Ethernet.

So percentage of time used in monitoring stations = $\frac{1.6}{50} \times 100 = 3.2\%$.

What would the percentage be if the inter-frame gap were to be taken into account?

Example 2

It has been decided to remotely monitor the connectivity of 600 networked devices. The polling station connects via a 100 Mbps full duplex fast Ethernet connection.



Determine the fastest rate at which a device can be polled if no more than 0.1% of the capacity of the link is to be used in polling.

Hints: What is the minimum size of ICMP echo request and echo reply messages? What is the minimum size of an ethernet frame? The inter-frame gap in 100 Mbps Ethernet is 960 ns.

[\approx once every 4 s]

Minimum size of an ICMP echo request/reply message = 8 bytes. IP header = 20 bytes.
So minimum size ping packet = 28 bytes.

```
johnh@hardy:~$ ping -s 0 -c 1 149.170.13.7
PING 149.170.13.7 (149.170.13.7) 0(28) bytes of data.
8 bytes from 149.170.13.7: icmp_seq=1 ttl=64
```

Minimum size of data in Ethernet frame = 46 bytes. Since this is more than the minimum size ping packet the packet would be padded with 18 bytes, and would be carried in a minimum size Ethernet frame of 72 bytes.

Since communications is full duplex only transmission (or reception) need be considered.

Time taken to transmit 600 minimum size Ethernet frames on 100 Mbps Ethernet

$$= 600 \left(\frac{72 \times 8}{100 \times 10^6} + 960 \times 10^{-9} \right) = 4.032 \text{ ms}$$

If T is the time between successive polls of the devices $\frac{4.032 \times 10^{-3}}{T} = \frac{1}{1000}$

So T, the polling interval = $1000 \times 4.0 \times 10^{-3} \approx 4 \text{ s}$

(b) Discuss the usefulness of implementing each of the five functional areas of network management in a network consisting of about 200 nodes on 6 subnets on a single site in a department of an academic institution where most of the nodes are machines used for teaching purposes. [6]

(c) A network administrator responsible for a small network of machines **all** running Linux wishes to find out who is logged into the network at a machine's terminal and also remotely logged in by using a shell script. Produce a **design** for a script to perform this task.

You may assume that all machines are permanently left on and that the IP addresses of all machines on the network are stored in the first column of each line of the file `/etc/hosts`. You may also assume that `ssh` (secure shell) has been configured to allow execution of a command on a remote host without being prompted for a password. All users whose idle terminal period is marked as old should be excluded from the list of users logged in. See the additional information sheet for more information about the `who` command. [9]